

Affidavit in Support of Search Warrant Application

I, Todd Matney, being duly sworn, depose and say:

I have been a duly authorized Postal Inspector with the United States Postal Inspection Service for approximately 13 months. I am currently assigned to the U.S. Postal Inspection Service Domicile in Oxford, Mississippi. Pursuant to Title 18, United States Code, Section 3061, my duties include the investigation of crimes that may have a nexus or link to the U.S. Postal Service. I have previously investigated instances of robbery and assault of federal employees. I have received training in the investigation of these crimes at the Federal Law Enforcement Training Center, the U.S. Secret Service training academy and the U.S. Postal Inspection Service training academy. During my law enforcement career, which includes approximately 10 plus years as a police officer, approximately 10 plus years as a Special Agent with the U.S. Secret Service and approximately three years as a Special Agent with U.S. Postal Service Office of Inspector General, I have attended numerous training classes covering a wide range of investigative techniques.

INTRODUCTION

1. This affidavit is made in support of an application for a search warrant for information that is maintained on computer servers controlled by Google, Inc. ("Google"), an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Section I of Attachment A, which consists of Google location data associated with a particular specified location at a particular time, as specified in Section I of Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. section 2703(c)(1)(A) to require Google to disclose to the government copies of the information further described in Section II of Attachment A.

Exhibit "B"

2. Based on the facts set forth in this affidavit, there is probable cause to believe that the Google accounts identified in Section I of Attachment A, associated with a particular specified location at a particular specified time, contain evidence, fruits and instrumentalities of a violation of 18 U.S.C. section 2114(a), Robbery of a U.S. Postal Service Employee. This affidavit is based upon my personal knowledge, my review of documents and other evidence, and my conversations with other law enforcement officers, as well as my training and experience concerning the use of email in criminal activity. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts I have learned during my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

JURISDICTION AND AUTHORITY TO ISSUE WARRANT

3. Pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as the Provider, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

4. A search warrant under § 2703 may be issued by “any district court of the United States (including a magistrate judge of such a court)” that “has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

5. When the Government obtains records under § 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2) & (3). Additionally, the Government may obtain an order precluding the Provider from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

**BACKGROUND RELATING TO GOOGLE, GOOGLE LOCATIONS SERVICES
AND RELEVANT TECHNOLOGY**

6. A cellular telephone or mobile telephone is a handheld wireless device primarily used for voice, text, and data communication through radio signals. Cellular telephones send signals through networks of transmitter/receivers called “cells,” enabling communication with other cellular telephones or traditional “landline” telephones. Cellular telephones rely on cellular towers, the location of which may provide information on the location of the subject telephone. Cellular telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

7. Google is a company which, among other things, provides electronic communication services to subscribers, including email services. Google allows subscribers to obtain email accounts at the domain name gmail.com and/or google.com. Subscribers obtain an account by registering with Google. A subscriber using the Provider’s services can access his or her email account from any computer connected to the Internet.

8. Google has developed an operating system for mobile devices, including cellular phones, known as Android, which has a proprietary operating system. Nearly every cellular phone using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device. Based on my training and experience, I have learned that Google collects and retains location data from Android-enabled mobile devices when a Google account user has enabled Google location services. Google can also collect location data from non-Android devices if the device is registered to a Google account and the user has location services enabled. The company uses this information for location-based advertising and location-based search results. This location information is derived from GPS data, cell site/cell tower information, and Wi-Fi access points.

9. Location data can assist investigators in understanding a fuller geographic picture and timeline, which may tend to identify potential witnesses, as well as possibly inculcating or exculpating account owners. Additionally, location information digitally integrated into image, video, or other computer files sent via email can further indicate

the geographic location of the accounts user at a particular time (e.g., digital cameras, including on cellular telephones, frequently store GPS coordinates indicating where a photo was taken in the metadata of image file).

PROBABLE CAUSE STATEMENT

10. Sylvester Cobbs works as a U.S. Postal Service Highway Contract Route driver. Cobbs' duties include picking up the mail from the Dundee, Tunica, Robinsonville, Lake Cormorant, and Walls, Mississippi Post Offices and transporting that mail to the Processing and Distribution Center in Memphis, Tennessee.

11. On February 5, 2018, at or around 5:25 p.m., Cobbs was performing his official duties, in a truck clearly marked "U.S. Mail," by picking up the mail from the Lake Cormorant Post Office, located at 12744 Star Landing Road West, Lake Cormorant, MS 38641, which is located in Desoto County, Mississippi.

12. While parked in the parking lot of the Lake Cormorant Post Office, Cobbs was approached from behind by an African-American male subject described as being approximately 5'9" to 6'0" tall, wearing a black long sleeve shirt and a black ski mask.

13. Postal Inspectors interviewed Cobbs who stated he was approached from behind by the subject who pointed a handgun with one hand and had some form of mace in the other hand. The subject told Cobbs he would shoot him. The subject tried to lock Cobbs inside the vestibule of the post office. Cobbs fought back with the subject and was ultimately pistol whipped several times in the parking lot. The subject went to the rear of the mail truck and stole three registered mail sacks and Cobbs' keys to the post offices. Cobbs said the subject walked to the rear of the truck and took exactly what he was looking for, as if he knew what was in the bags.

14. Cobbs reported the subject walked away. Cobbs stated he drove his truck across the street where he called his wife, then postal management. Later that night, Cobbs sought medical treatment for his injuries. Cobbs reported he saw a new model dark red or maroon Hyundai vehicle in the area before the robbery.

15. In the days following the robbery, Postal Inspectors located surveillance footage from a nearby farm which captured the robbery on video. The video surveillance not only showed a maroon Hyundai, believed to be an Elantra, but also a large white

SUV; this vehicle is believed to be a newer model GMC Yukon XL. The subject was seen on video getting out of the GMC Yukon prior to the robbery. Additionally, based on a review of the video, it is reasonable to conclude the subject got back into the white SUV upon fleeing the scene.

16. Postal Inspectors conducted a detailed review of the video surveillance and it appears the robbery suspect is possibly using a cellular device both before and after the robbery occurs.

17. The investigation revealed that the subjects stole three registered mail sacks from Dundee, MS 38680; Tunica, MS 38676; and Robinsonville, MS 38664 Post Offices; the total of all the remittances was about \$60,706.

18. Based on my training and experience, this was a premeditated crime that took the knowledge of planning of multiple offenders. Based on the amount of U.S. Currency that was contained in the registered mail sacks; the behavior of the suspect vehicles; and the subject fleeing the scene in a similar vehicle, shows the likelihood that cell phones were used for talking on the phone or sending other digital messages such as but not limited to text messages and/or emails. I believe this information will assist in determining who planned, surveilled, and/or committed the robbery of Sylvester Cobbs and/or may assist in locating additional witnesses.

EVIDENCE, FRUITS AND INSTRUMENTALITIES

19. Based on the foregoing, I respectfully submit that there is probable cause to believe that information stored on the Providers' servers associated with the Google accounts accessed at particular specified location at a particular specified time, as specified in Section I of Attachment A of the proposed warrant, will contain evidence, fruits and instrumentalities of the Subject Offenses.

20. In particular, the geographical region bounded by the latitudinal and longitudinal coordinates indicated in Section I of Attachment A and the time specified in Section I of Attachment A to the proposed warrant reflects the period between 5:00 p.m. CT and 6:00 p.m. CT on February 5, 2018. The specific longitude and latitude indicated in Attachment A was identified through the use of mapping software, which matched the longitude and latitude indicated in Attachment A as corresponding to the area of Latitude

34.90467 Longitude -90.216485 where the robbery took place (Lake Cormorant, MS Post Office). This Application seeks authority to collect certain location information related to Google accounts that were located within the Target Area during the Target Time Period (the "Subject Accounts").

21. The information sought from Google regarding the Subject Accounts, specified in Section II of Attachment A to the proposed warrant, will identify which cellular devices were near the location where the robbery took place and may assist law enforcement in determining which persons were present or involved with the robbery under investigation. The requested information includes:

a. *Location information.* All location data, whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, and precision measurement information such as timing advance or per call measurement data, and Wi-Fi location, including the GPS coordinates, estimated radius, and the dates and times of all location recordings, during the Target Time Period;

b. Each device corresponding to the location data to be provided by Google will be identified only by a numerical identifier, without any further content or information identifying the user of a particular device. Law enforcement will analyze this location data to identify users who may have witnessed or participated in the Subject Offenses and will seek any additional information regarding those devices through further legal process.

REQUEST FOR NON-DISCLOSURE AND SEALING

22. Based on the forgoing, I respectfully request that the Court issue the proposed search warrant. Because the warrant will be served on Google who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

23. The scope of this ongoing criminal investigation is not publicly known. As a result, premature public disclosure of this affidavit or the requested warrant could alert potential criminal targets that they are under investigation, causing them to destroy evidence, flee from prosecution, or otherwise seriously jeopardize the investigation. In light of the violent nature of the crime under investigation, premature revelation of this

investigation may alert dangerous targets that they have been identified by others.

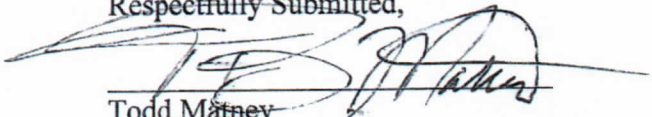
24. Accordingly, there is reason to believe that, were the Provider to notify subscribers of the Subject Accounts or others of the existence of the warrant, the investigation would be seriously jeopardized. Pursuant to 18 U.S.C. § 2705(b), I therefore respectfully request that the Court direct the Provider not to notify any person of the existence of the warrant for a period of 180 days from issuance, subject to extension upon application to the Court, if necessary.

25. For similar reasons, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

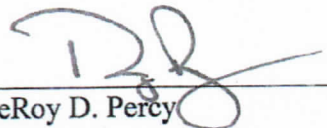
CONCLUSION

26. Based on the foregoing, I respectfully request that the warrant sought herein pursuant to the applicable provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) (for contents) and § 2703(c)(1)(A) (for records and other information), and the relevant provisions of Federal Rule of Criminal Procedure 41.

Respectfully Submitted,


Todd Matney
United States Postal Inspector

Sworn and subscribed before me on this 8th day of Nov., 2018.


LeRoy D. Percy
U.S. Magistrate Judge

ATTACHMENT A

I. Subject Accounts and Execution of Warrant

This warrant is directed to Google, Inc. (the "Provider"), headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043, and applies to all content and other information within the Provider's possession, custody, or control associated with the Google accounts located within the geographical region bounded by the following latitudinal and longitudinal coordinates between 5:00 p.m. CT and 6:00 p.m. CT on February 5, 2018 (the "Subject Accounts"):

Geographical box with the following 4 (four) latitude and longitude coordinates:

- 1). NW: 34.906562, -90.21698
- 2). SW: 34.903791, -90.217003
- 3). NE: 34.906574, -90.213449
- 4). SE: 34.903816, -90.213441

The highlighted area in the below map is the area represented by the coordinates listed above and the location pinned in the middle of the highlighted area is the location of the Lake Cormorant Post Office.

